OGeek · 即刻不凡

oppo

情报驱动的安全运营体系

基于腾讯云的安全运营实践

- 关于我
- 为什么做情报
- 情报驱动的安全运营体系

01 关于我

关于云鼎实验室

腾讯安全云鼎实验室专注云安全技术研究和云安全产品创新工作；负责腾讯云安全架构设计、腾讯云安全防护和运营工作；通过攻防对抗、合规审计搭建管控体系，提升腾讯云整体安全能力。

腾讯安全云鼎实验室
TENCENT SECURITY YUNDING LAB

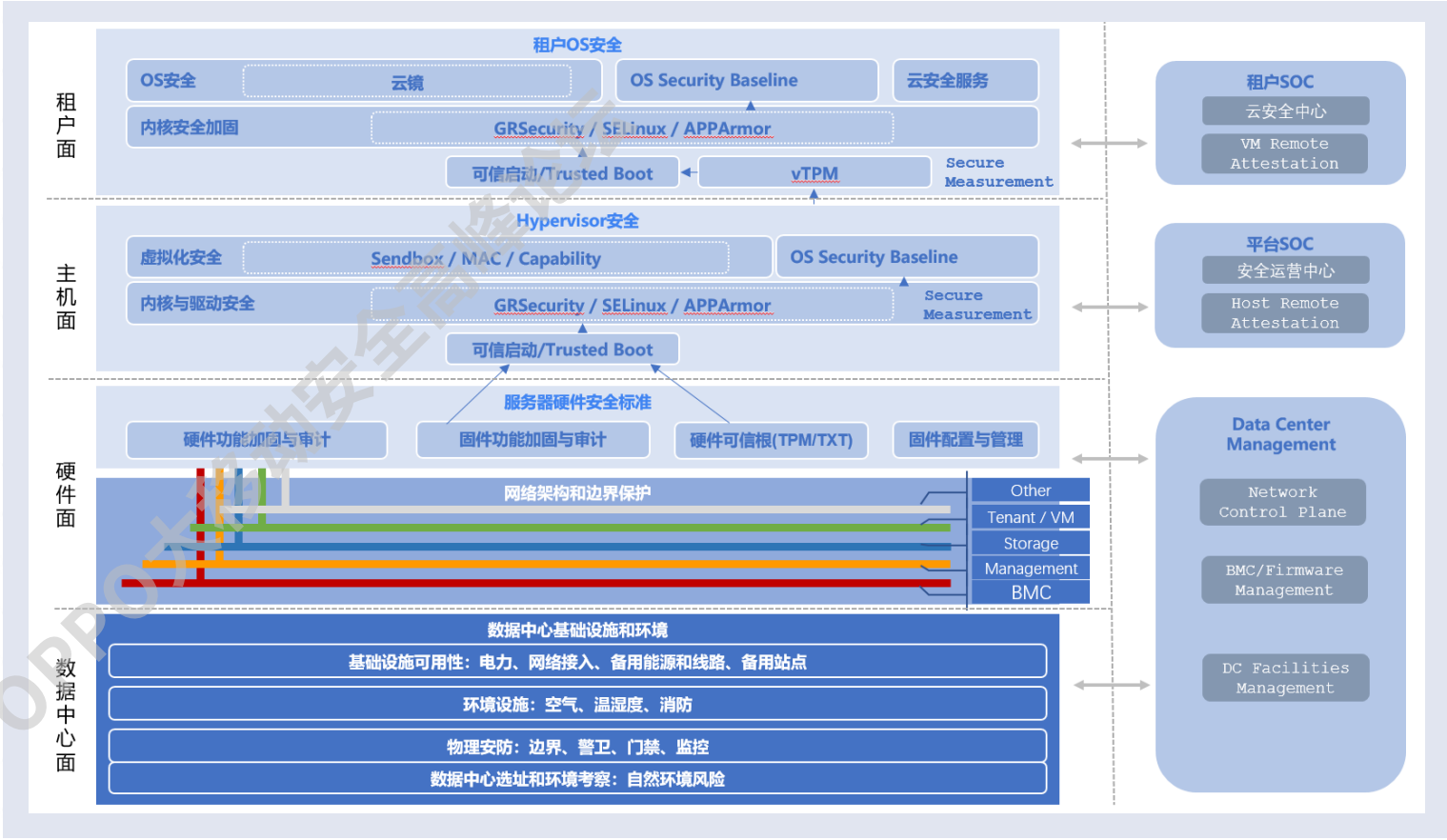


图 腾讯云全栈安全基础设施

02 为什么做情报

2017年"永恒之蓝"漏洞爆发，肆虐全球

- 5月12日，WannaCry蠕虫病毒在**互联网上大肆爆发**
- 影响到全球 **近百个国家上千家企业** 及公共组织
- 社交媒体微信、微博、科技媒体、安全媒体、博客等**快速传播发酵**

团队对"永恒之蓝"漏洞的复盘思考

重大漏洞来临，云服务商需要做什么，从哪里开始做，如何评价做得好不好?

①如何更快发现，并提醒业务做好防范?

②修复时间 VS 系统稳定性 平衡?

③云环境下修复对象包含哪些?

④修复指标如何衡量?

⑤针对批量利用，如何快速止损?

⑥已中招用户如何引导修复?

⑦外部安全舆情危机及内部询问，如何应对?

……

"永恒之蓝"漏洞应急响应启示——时间窗口

时间 × 效率 × 指标

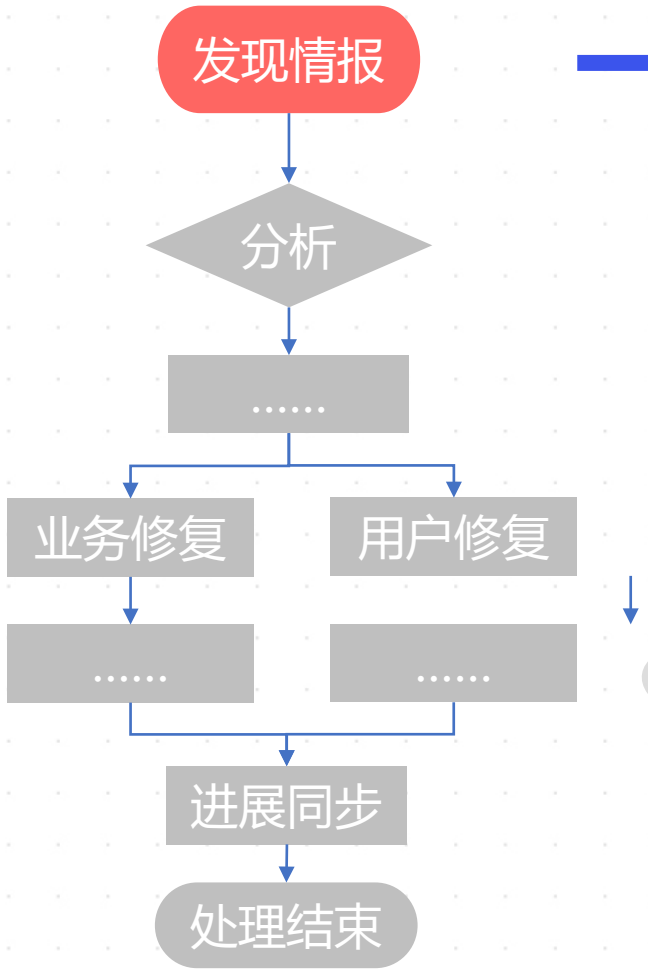
（漏洞发现） × （流程规范工具） × （审计手段）

（事前响应） × （事中处理） × （事后优化）

那么，如何跟黑客赛跑，争取更大的时间窗口？

情报是扩大时间窗口的核心武器

只有知道外部新出现哪些漏洞或威胁，才能第一时间启动应急响应，为业务预留更多修复时间窗口

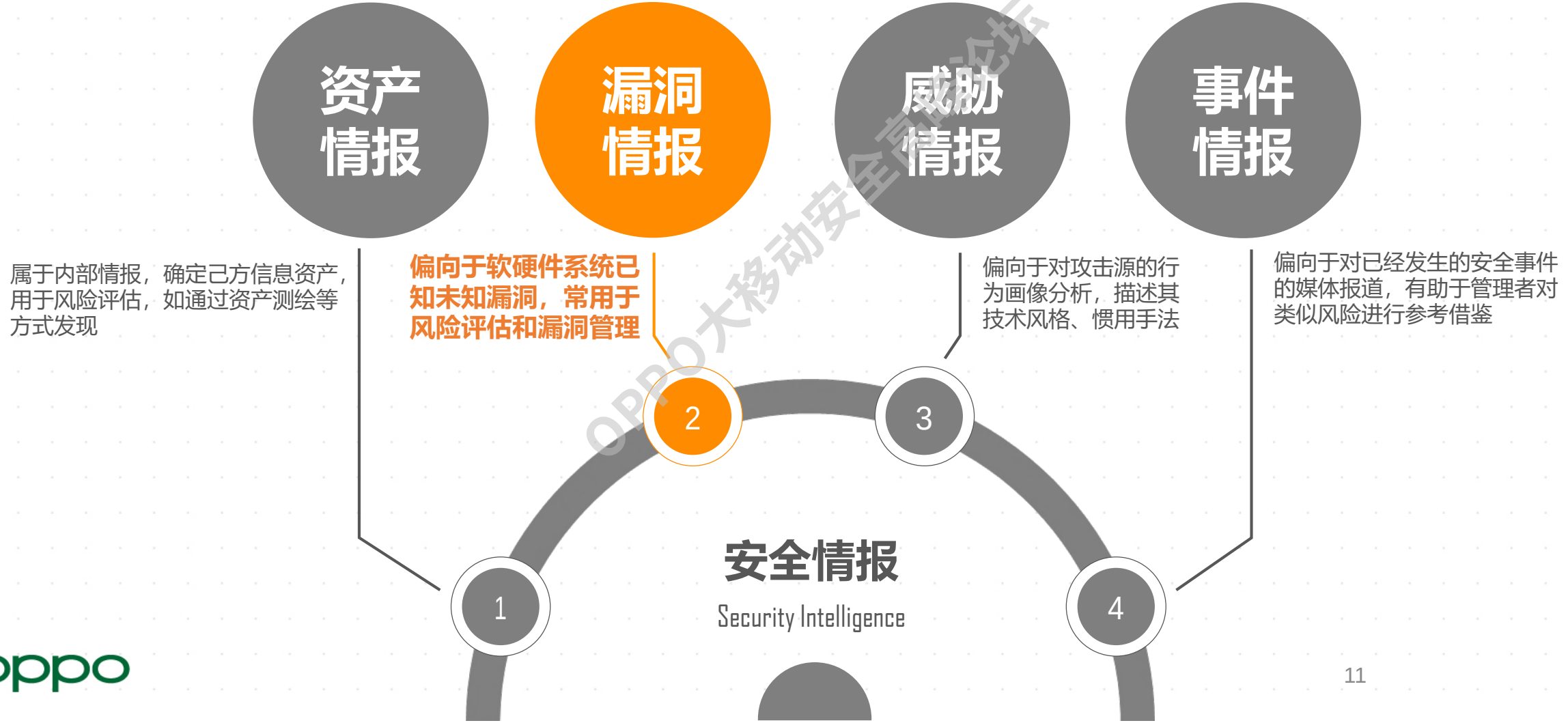


情报价值

- **了解最新漏洞态势**
  - 外界有什么风险?
  - 风险影响是什么?
  - 目前有没有利用工具?
  - 修复方案是什么?
  - 有没有人已被入侵了?
- **触发应急响应流程**
- **完善安全防护策略**
- **辅助应对外部安全舆情**

03 情报驱动的安全运营实践

对安全情报的理解



如何获取最新的漏洞情报——了解漏洞的生命周期

OGeek

漏洞出生 → 漏洞成长 → 漏洞爆发 → 漏洞死亡

- **关键标识：**
  - **CVE申请**
  - **社区邮件列表**
  - **官方公告**
  - **安全博客**

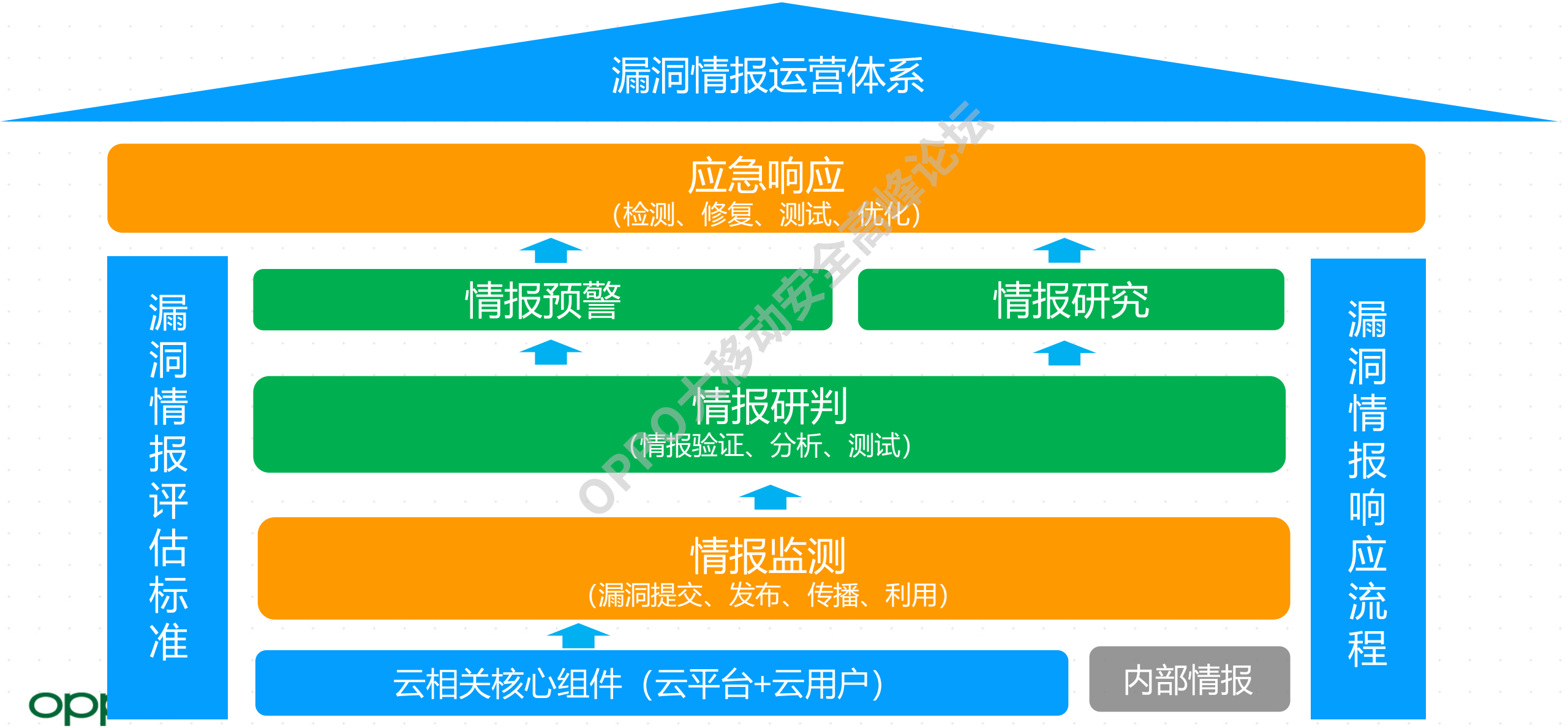
- **关键标识：**
  - **开源社区**
  - **漏洞细节**
  - **公开PoC**

- **关键标识：**
  - **自动化工具**
  - **大规模传播**
  - **媒体报道**

- **关键标识：**
  - **技术分析**
  - **淡出视野**

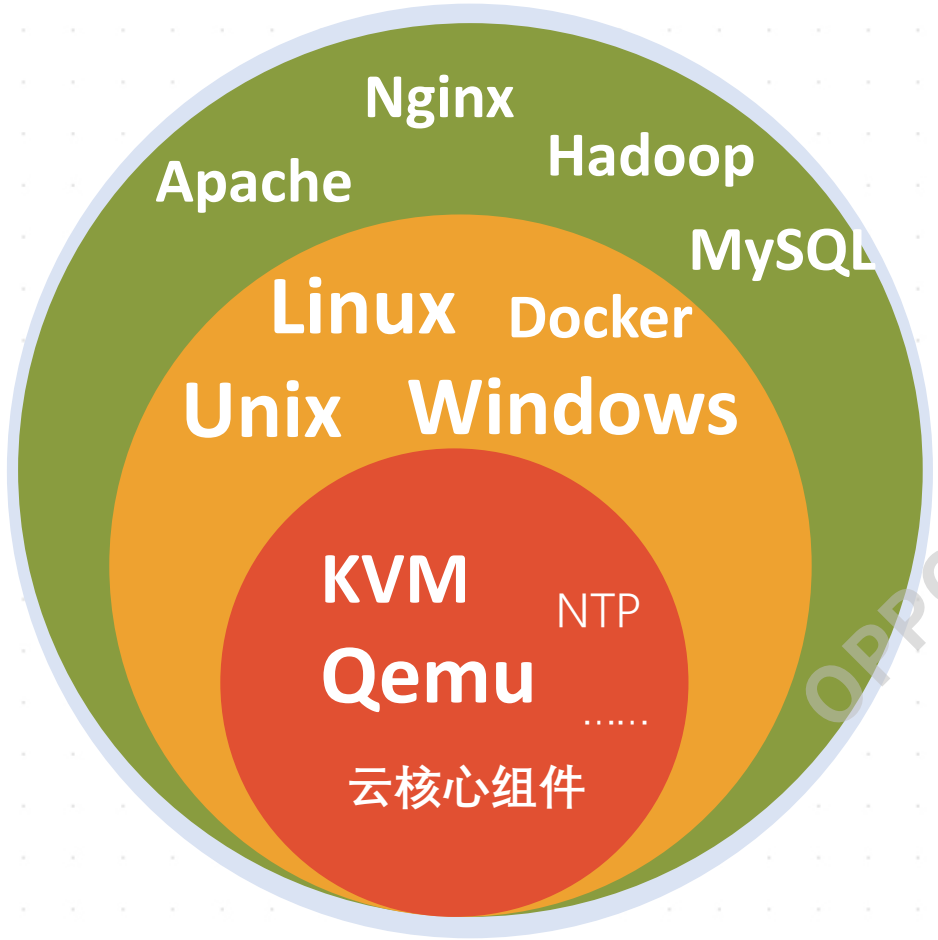
oppo

漏洞情报体系设计思路



关于监控目标的选择——定位云相关核心组件

基于数百次重大漏洞应急总结，梳理出云相关核心系统或组件，建立核心资产**漏洞监测列表（110+）**



情报监测：分析维护一手情报渠道，高频捕获

OGeek

300+情报源，21种渠道类型，30分钟全渠道捕获

社交网络发布

漏洞作者或团队发布

公众号发布

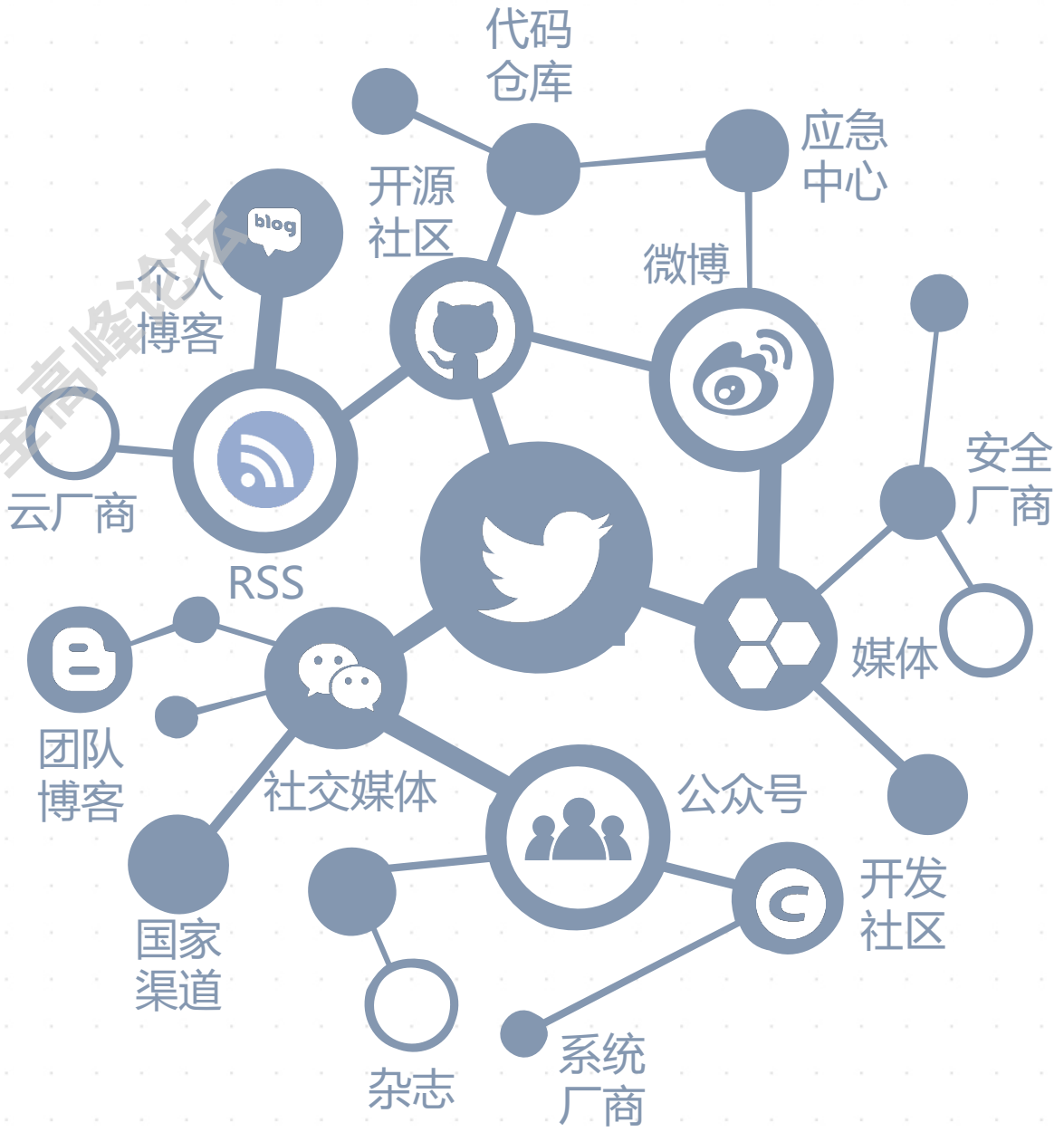
官方或组件厂商发布

安全厂商发布

新闻媒体发布

外部获取的漏洞情报源

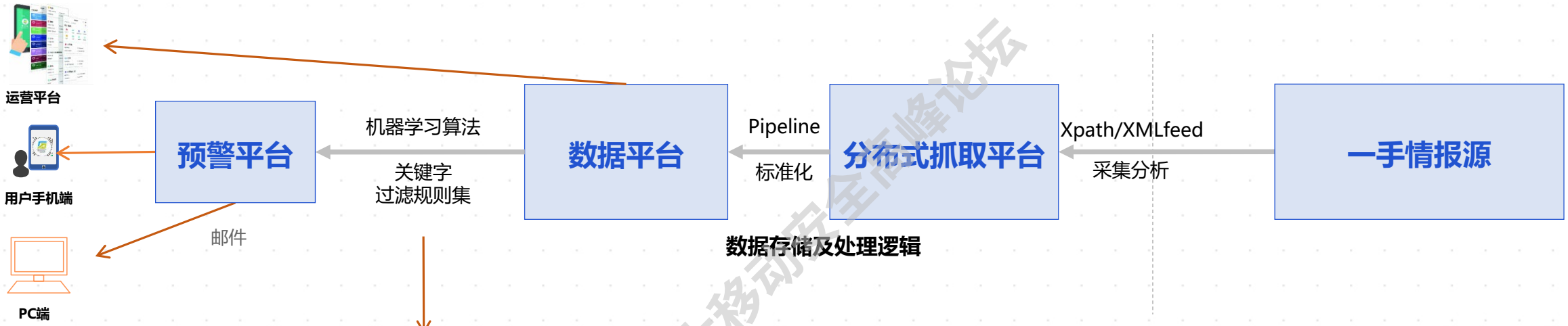
掌握历史漏洞作者或团队的漏洞发布位置并进行捕获，是获取一手情报源的关键



oppo

技术实现：基于开源爬虫框架设计，高扩展，稳定性强

系统每周可以捕获到6000多个情报，经过自动化过滤，可以筛选出400左右的目标情报



过滤规则集

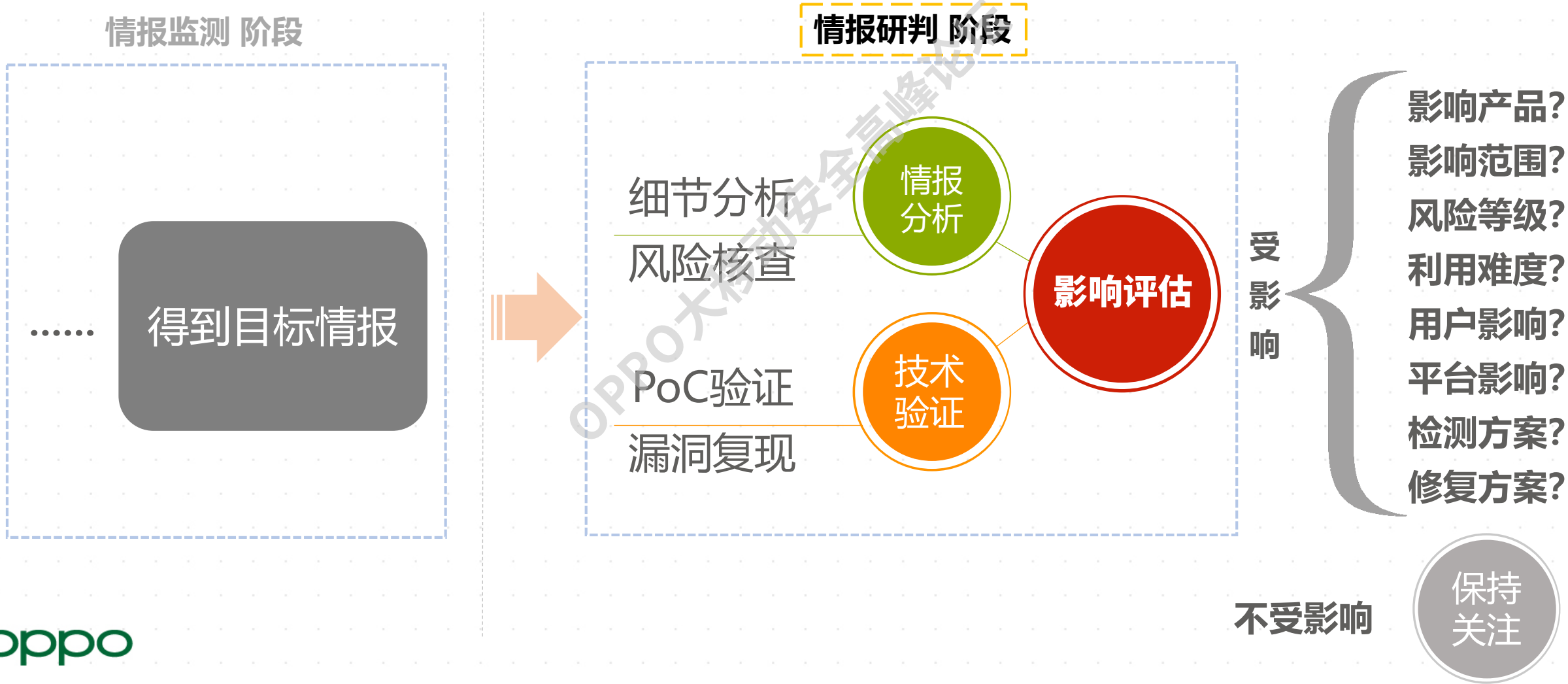
- 资产组件库
- 漏洞关键字库
- 情报源权威值
- 非重点黑名单
- 机器学习

设计思路

- **稳定可靠**：选取稳定爬虫平台，无性能问题
- **支持扩展**：新情报源，可以轻松扩容
- **具备反爬**：具备一定抗反爬能力，UA、IP代理、Splash
- **及时告警**：短信+邮件，手机端、PC都能快速看到
- **数据共享**：漏洞数据标准化，输出给运营平台
- **失效监控**：具备情报源失效监控能力

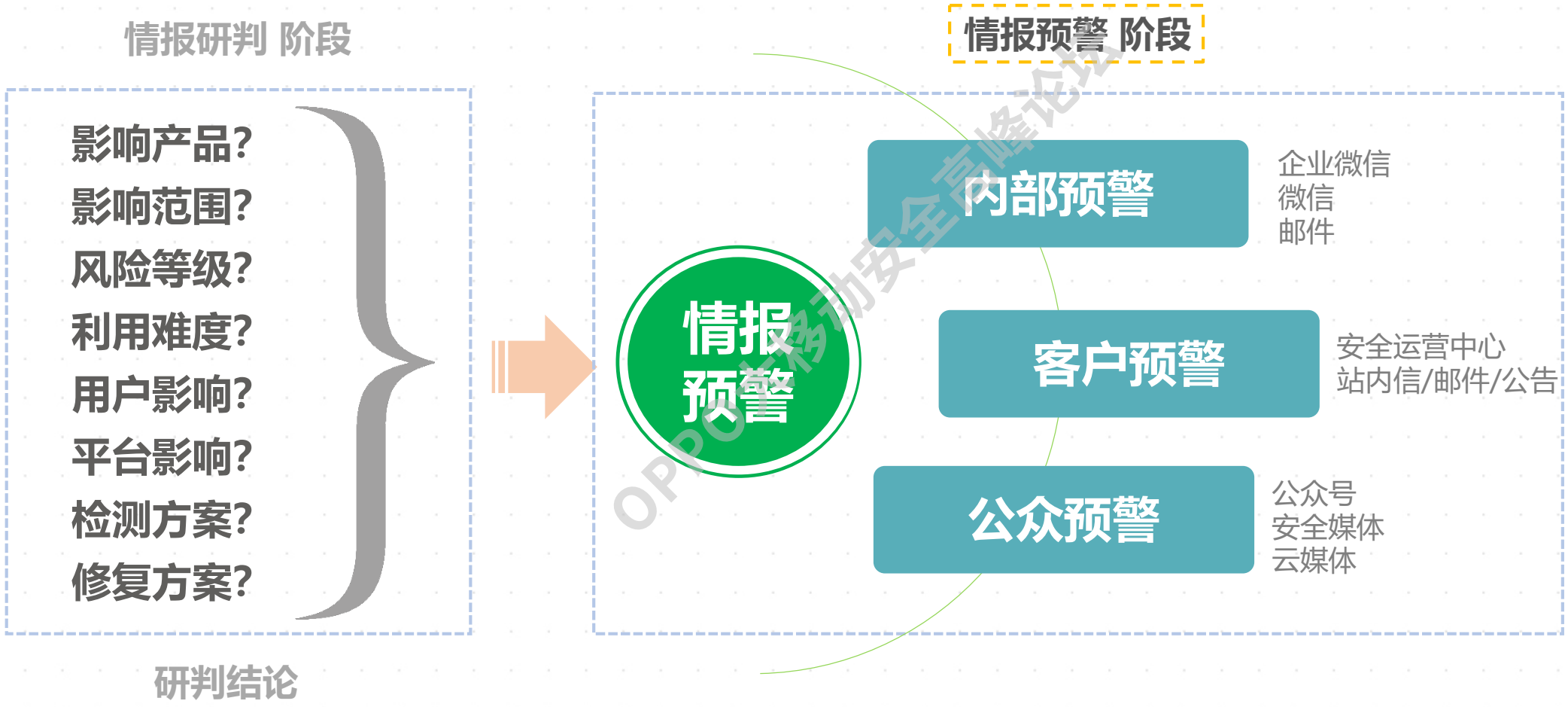
情报研判：整个情报运营体系中最重要的一步

从原始情报提取出价值情报，除过滤规则库外，还需要人工介入进展**技术分析、验证测试**，确认情报程度及影响面



情报预警：对内和对外提供多种预警方式

确认价值情报后，进入 **情报预警** 阶段，知会相关风险及修复建议给相应团队及用户，进入应急响应控制风险



情报研究：针对基础设施或通用问题进行专题研究

结合情报对基础设施（固件、容器服务、虚拟化服务等）的影响范围和危害程度，进行专项深度研究

情报研判 阶段

影响产品?
影响范围?
风险等级?
利用难度?
用户影响?
平台影响?
检测方案?
修复方案?

研判结论

影响核心基础设施？

情报专题研究

- 基础固件
- 容器服务
- 虚拟化组件
- ……

以点带面，系统研究

专题研究

应急响应：为内外部事件处置提供运营决策支撑

应急响应 即情报的深度赋能阶段，通过监控漏洞利用、传播、事件态势，为内部响应修复提供运营决策指导

情报运营过程中的挑战与解决手段

情报运营重点解决两类问题：
1、**系统误报漏报优化**，针对漏报、误报情况，完善情报源并优化相关规则
2、**持续监控利用**，监控漏洞利用传播情况，调整修复策略

典型问题

- 漏报
- 误报
- 反爬
- 情报源失效
- ……

情报运营

情报运营 阶段

漏报解决	查漏补缺，新增情报源或规则完善
误报解决	调整策略，优化情报监测规则
反爬措施	持续对抗，了解网站反爬规则
失效解决	反向验证，监控后开发新爬虫
… 运营	持续利用监控，变种舆情监控 ……

情报腾讯云安全运营中心对外输出

OGeek

THANKS

OPPO大移动安全高峰论坛

oppo